TP3
Implémentation du SSL sur le serveur HTTP Apache2

1 Objectif

Passer du HTTP au HTTPS en utilisant un outil SSL et s'habituer à la gestion des certificats

2 Le SSL - Secure Socket Layer

Le *SSL* est un protocole de sécurisation des échanges sur Internet, développé à l'origine par Netscape (SSL version 2 et SSL version 3) ...[1].

3 Le serveur apache

Le logiciel libre Apache HTTP Server (Apache) est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web. Il est distribué selon les termes de la licence Apache[2].

4 Plateforme du TP

Pour la réalisation de ce tp, on va adopter la plateforme illustrée au schéma suivant:

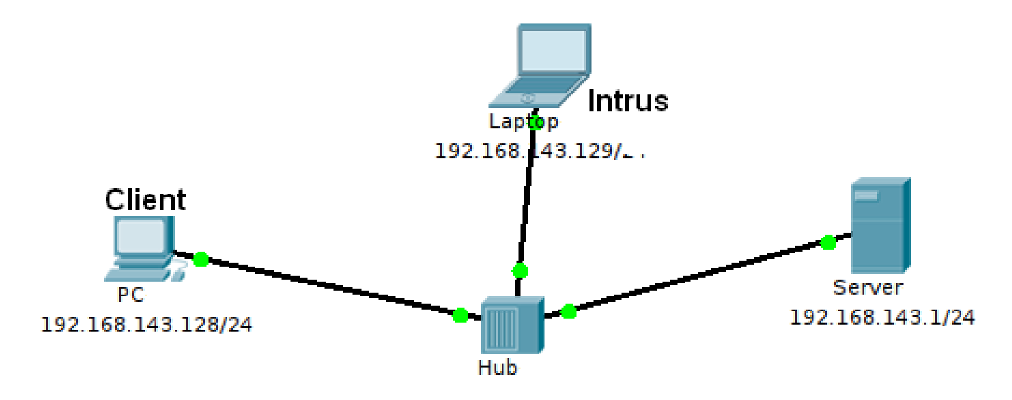


Figure 1: Réseau LAN

5 Écoute du trafic HTTP

- Lancez le *wireshark* sur l'ordinateur "intrus"
- Sur la machine cliente, lancez votre navigateur web et appliquer une requête *HTTP* vers le serveur
- Analysez ce trafic

[1] Wikipédia
[2] Wikipédia

6 Activer le SSL

- Exécutez les commandes suivantes:
  - sudo a2enmod ssl
  - sudo a2ensite default-ssl
  - sudo service apache2 restart
- réanalysez un trafic *HTTP*
- vérifiez l'identité du site et de son certificat numérique

7 Générer un certificat auto-signé

- Déplacez vous au dossier ssl.ca-0.1[3]
- Exécutez new-root-ca.sh (pour la création d'une CA privée. Un mot de passe sera demandé et va nous servir pour signer les certificats numériques)
- Créez un certificat numérique pour le serveur en exécutant new-server-cert.sh (le nom du serveur web sera donné comme paramètre au script)
- Lancez le script *sign-server-cert.sh* pour signer le certificat
- Mettez les clés du serveur dans le dossier /etc/apache2/ssl-certs
- Éditez le fichier /etc/apache2/sites-available/default-ssl

  SSLCertificateFile /etc/apache2/ssl-certs/localhost.crt

  SSLCertificateKeyFile /etc/apache2/ssl-certs/localhost.key
- Redémarrez le serveur apache2

[3] http://www.openssl.org/contrib